RAISECOM

www.raisecom.com

DHCP Configuration Guide

Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of

Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road, Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

http://www.raisecom.com

Feedback

Comments and questions about how the … system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

http://www.raisecom.com/en/xcontactus/contactus.htm.

If you have comments on the … specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of … device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《… User Manual》

《… Commands Notebook》

Organization

This manual is an introduction of the main functions of … EMS. To have a quick grasp of the using of the EMS of … , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of …

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the ….

Chapter 3 Performance Management

This chapter focuses on performance management function of ….

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of ….

Appendix A Alarm Type

The alarm types supported by ….

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 System Overview

This chapter is mainly about how to configure and maintain DHCP snooping on switches, which includes:

- ✧ DHCP Snooping principle
- ✧ DHCP Snooping configuration
- ✧ Monitoring and maintenance
- ✧ DHCP Snooping trouble shooting

1.1 DHCP Snooping principle

Introduction:

If there is private DHCP server in the network, user may get wrong IP address. DHCP Snooping is a safe feature of DHCP, it provides network safety by filtrating the unbelievable DHCP message and establishing and maintaining a DHCP Snooping binding database (or DHCP Snooping binding table). To let user get IP address from valid DHCP server, DHCP Snooping safety mechanism allows the port to be set to creditable port and unauthentic port. It divides creditable port from unauthentic port on the switch, filtrates the unauthentic DHCP response message to insure the network safety. It is like firewall between unauthentic host and DHCP server.

Unauthentic DHCP message is the message that the host received from the network or outside the firewall. When DHCP Snooping is used in the network that provides network services, unauthentic message is from other network which does not belong to the server network, like user switch. The messages that are from unknown equipments may be attacking source, so it is unauthentic. At the same time, to make sure the network safety, network administrator may need to record the user’s IP address when user is online, to make sure the correspondence relationship between the IP address that user gets from DHCP server and user host MAC address. By monitoring DHCP Request and DHCP ACK broadcast message received by the creditable port, DHCP Snooping records the client MAC address and the IP address acquired to actualize the function.

In the network that provides services, the creditable port is connected with DHCP server; the unauthentic port is connected with client side, or with other equipments in the network. The unauthentic port will drop the DHCP-ACK, DHCP-NAK and DHCP-OFFER message that is received from DHCP response (because these equipments that are connected with unauthentic ports should not make any response to DHCP server); while the response message received b the creditable port will be transmitted normally, which will prevent pseudo-server deception and make sure that user can get the correct IP address.

Fig 1-1 is a typical network picture of DHCP Snooping:

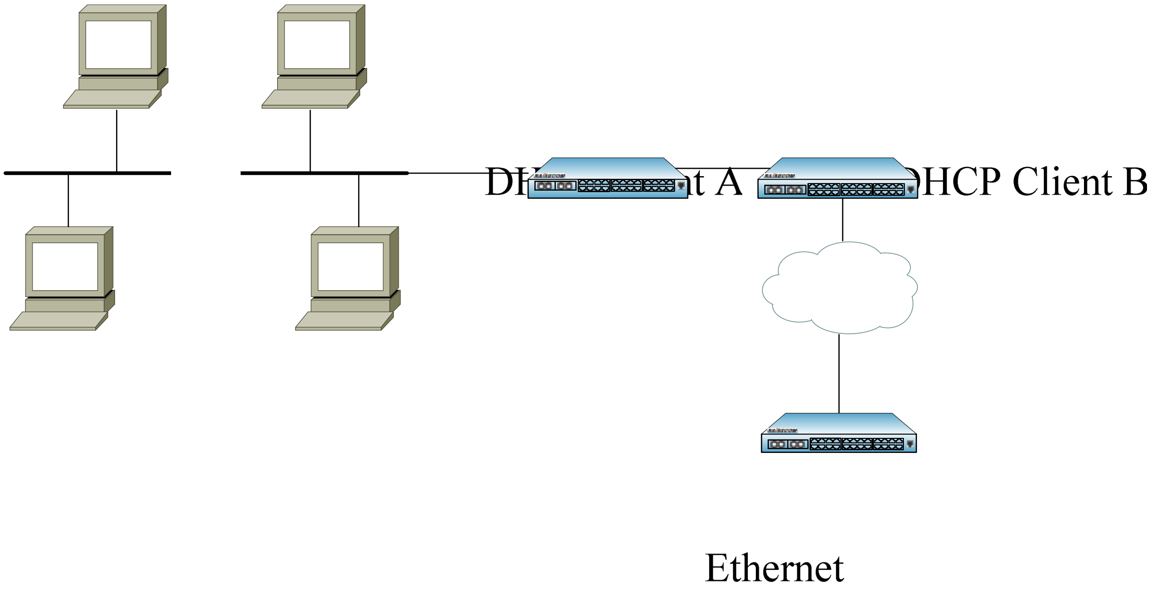

Fig 1-1 DHCP Snooping typical network structure

Option 82 overview:

Option 82 is the Relay Agent Information option of DHCP message, which is identified in request document RFC3046. When DHCP Client sent request message to DHCP Server, if it is needed to cross DHCP Snooping, DHCP Snooping will add Option 82 to request message. Option 82 contains much sub-option. The option 82 introduced here support sub-option 1 and sub-option 2:

sub-option 1: circuit ID is defined in it

sub-option 2: remote ID is defined in it

sub-option 1: sub-option 1 is a sub-option of Option 82, which is circuit ID sub-option. A sub-option is usually configured on DHCP Snooping equipment or repeaters, which defines the port number of the switch port that needs to carry DHCP client when transmitting messages and the port's VLAN number. Usually sub-option1 and sub-option 2 need to be used together to note the information of DHCP source port.

Sub-option 2: it is also a sub-option of Option 82, which is Remote ID. This sub-option is usually also configured on DHCP repeater, which defines the MAC address information of the equipments that carry Snooping or repeater equipment. Usually sub-option 1 needs to be used together to note DHCP source port information.

Option 82 actualize the address information of DHCP client and DHCP snooping equipment or repeater equipment's record on DHCP server, with the help of other software it could actualize DHCP distribution restriction and billing function. For example, combined with IP Source Guard, the reception of IP address + MAC address can be defended effectively.

Option 82 handling actions:

1: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be added and transmitted.

2: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be transmitted; if not, the message will be dropped.

3: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be deleted and transmitted; if not, the message will be dropped.

The structure of Option 82 message:

Option 82 obeys ‘TLV’ option format, fig 1-2 shows its message structure:

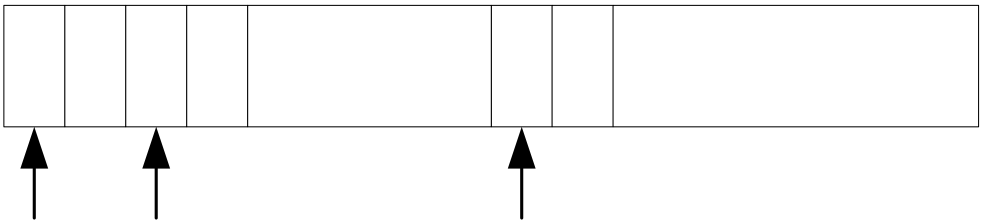

Fig 1-2 Option 82 message structure

1.2 Configure DHCP Snooping

The part describes how to configure DHCP Snooping on the switch, including:

- Default DHCP Snooping configuration
- DHCP Snooping configuration guide
- Global DHCP Snooping configuration
- Port trust configuration
- DHCP Snooping supporting Option 82 configuration

1.2.1 Default DHCP Snooping configuration

Function	Default value
Global DHCP Snooping state	Disabled
Port DHCP Snooping state	Enabled
Port trust state	Untrusted
DHCP Snooping supporting Option 82	Disabled

1.2.2 DHCP Snooping configuration guide

1. Make sure that the switch DHCP Server or DHCP Relay is not enabled;
2. Global DHCP Snooping must be enabled;
3. If DHCP Snooping is not enabled on the port, DHCP Snooping can not is not available on the switch;

4. After DHCP Snooping is on, DHCP Server or DHCP Relay can not be started on the switch;
5. If only DHCP Snooping is enabled, while DHCP Snooping supporting Option 82 is not, the switch will not insert Option 82 in the message nor handle the message that contains Option 82;
6. Make sure the port that connects DHCP server is credible, while the port that connects client side is incredible.

1.2.3 Configure global DHCP Snooping

By default, global DHCP Snooping is off. Only when global DHCP Snooping is enabled can the switch DHCP Snooping take effect. To enable global DHCP Snooping, take the following steps:

The configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp snooping**	Enable global DHCP Snooping
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp snooping**	Show DHCP Snooping configuration

⚠Notice:

If the switch enables DHCP Server or DHCP Relay, global DHCP Snooping can not be started. On the opposite, if the switch enables DHCP Snooping, DHCP Server or DHCP Relay can not be started.

Use global configuration command **no ip dhcp snooping** to disable global DHCP Snooping.

1.2.4 Configure port DHCP Snooping

By default, DHCP Snooping is on, use **no ip dhcp snooping port-list** to close port DHCP Snooping.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp snooping port-list** 4-9	Enable DHCP Snooping on port 4-9
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp snooping**	Show DHCP Snooping configuration

⚠ Notice:

- By default, all the ports' DHCP Snooping of the switch is on. But until global DHCP Snooping is on can they be available. That is to say, if global DHCP Snooping is off, and only port DHCP Snooping is on, DCHP Snooping can not take effect.

1.2.5 Configure port trust

Unauthentic port will drop DHCP-ACK, DHCP-NAK, DHCP-OFFER message received from DHCP server response (because these equipments connected by unauthentic ports should not make any DHCP server response). While the DHCP server response message received by credible port will be transmitted normally.

Credible port connects DHCP server or the ports of others switches, while unauthentic port connects user or network, which keeps away from server deception, and makes sure user can get the correct IP address.

Follow the steps below to set the designated port to credit port.

Step	Command	description
1	**config**	Enter global configuration mode
2	**interface port 15**	Enter port configuration mode
3	**ip dhcp snooping trust**	Configure credit port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp snooping**	Show DHCP Snooping configuration

⚠Notice:

- Only when port trust is started in global DHCP Snooping and the port has also started DHCP Snooping can it take effect. Use **no ip dhcp snooping turst** to set the port to unauthentic port.

In port configuration mode use **no ip dhcp snooping trust** to set the port to unauthentic port and delete it from trust port list.

1.2.6 Configure DHCP Snooping supporting Option 82

Following the steps below, user can enable DHCP Snooping supporting Option 82, and the switch will add Option 82 option into the DHCP request message that receives Option 82; delete Option 82 in the DHCP response message that contains Option 82. The received DHCP request message that contains Option 82 will be handled according to the configured strategy and transmitted, while to the response message that don’t contain Option 82 option, the switch will not take any action and transmit it directly.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp snooping information option**	Enable DHCP Snooping supporting Option 82
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp snooping**	Show DHCP Snooping configuration

⚠Notice:

- DHCP Snooping supporting Option 82 function is global, but it reacts on the port. It can be enable only in global DHCP Snooping, and only when the port start DHCP Snooping can Option 82 take effect on the port.

Use global configuration command **no ip dhcp snooping information option** to stop DHCP Snooping supporting Option 82.

1.3 Monitoring and maintaining

Use the command **show** to look over the switch DHCP Snooping running state and configuration state and help monitoring and maintaining.

Command	Description
show ip dhcp snooping	Show DHCP Snooping configuration

Use **show ip dhcp snooping** to show DHCP Snooping configuration information, including global DHCP Snooping state, if Option 82 is supported, port DHCP Snooping state and port trust. Specific steps are as follows:

```
Raisecom#show ip dhcp snooping
DHCP Snooping: Enabled
Option 82: Enabled

 Port   Enabled Status       Trusted
 -----------------------------------------
 1        enabled              no
 2        enabled              no
 3        enabled              no
 4        enabled              no
 5        enabled              no
 6        enabled              no
 7        enabled              no
 8        enabled              no
 9        enabled              no
 10       enabled              no
 11       enabled              no
 12       enabled              no
```

```
13      enabled             no
14      enabled             no
15      enabled             yes
16      enabled             no
17      enabled             no
18      enabled             no
19      enabled             no
20      enabled             no
21      enabled             no
22      enabled             no
23      enabled             no
24      enabled             no
25      enabled             no
26      enabled             no
```

1.4 Typical configuration example

This part gives a introduction to a example that a DHCP client connects DHCP server and get IP address dynamically through DHCP Snooping, it show the typical configuration of DHCP Snooping.

1. Configuration explaination:

   This example is a simple and typical DHCP configuration, the two DHCP clients use DHCP port 2, 3 respectively to connect DHCP server.

   (1) Configure the correct address pool on DHCP Server, and enable DHCP Server function globally.

   (2) Enable DHCP Snooping function globally on DHCP Snooping equipment, and enable DHCP Snooping on the port, set port 1 to credible port, and configure DHCP Snooping supporting Option 82, use the default strategy Replace to handle the request messages from client side.

2. Topology picture

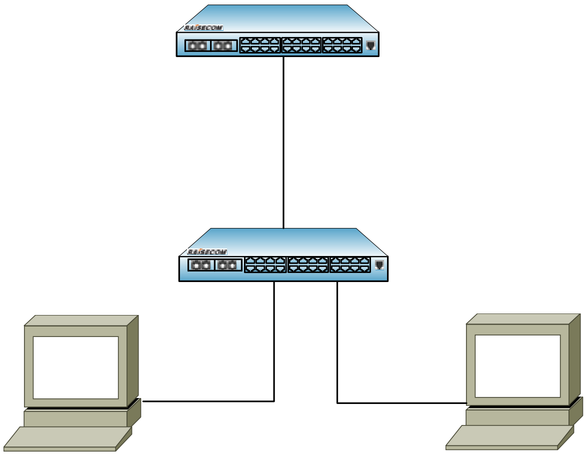

Fig 1-3 Typical DHCP Snooping configuration topology

3. Configuration step

Configure DHCP Snooping:

- Enable global DHCP Snooping:

```
Raisecom#config
Raisecom(config)#ip dhcp snooping
```

- Port enable DHCP Snooping:

```
Raisecom(config)# ip dhcp snooping port-list 1-3
```

- Set port 3 to DHCP Snooping credible port:

```
Raisecom(config)# interface port 1
Raisecom(config_port)# ip dhcp snooping trust
```

- Enable DHCP Snooping supporting Option 82:

```
Raisecom(config)#ip dhcp snooping information option
```

4. Show the result

DHCP Client A

On ISCOM switch use command **show ip dhcp snooping** to look over the switch DHCP Snooping running state and configuration state, on the client side use **show ip dhcp client** to show client IP address application. Specific contents are as follows:

```
Raisecom#show ip dhcp snooping
DHCP Snooping: Enabled
Option 82: Enabled


        Port    Enabled Status        Trusted
```

```
                 ------------------------------------------
  1          enabled                    yes
  2          enabled                    no
                 3         enabled                    no
            …            …                        …

Raisecom#show ip dhcp client
           Hostname:                    raisecomFTTH
           Class-ID:                    raisecomFTTH-3.6.1025
Client-ID:                    raisecomFTTH-000e5e8a0798-IF0
Assigned IP Addr:           10.0.0.5
    Subnet mask:                 255.0.0.0
    Default Gateway:             10.0.0.1
    Client lease Starts:         Jan-01-2007 08:00:41
    Client lease Ends:            Jan-11-2007 11:00:41
    Client lease duration:       874800(sec)
    DHCP Server:                  10.100.0.1

    Tftp server name:           --
    Tftp server IP Addr:        10.168.0.205
    Startup_config filename: 2109.conf
```

1.5 DHCP snooping trouble shooting

If DHCP client can not get network address normally through DHCP Snooping, it may be one of the following situations:

- If global DHCP Snooping and port DHCP Snooping are enabled at the same time;
- If DHCP Snooping do not open Option 82 option, when DHCP Snooping receives the message that contains Option 82 it will be dropped directly;
- If DHCP Snooping Option 82 option is enabled, and the request message handling strategy is set to be DROP, then the messages that contain Option 82 will be dropped;
- If the port is not configured as DHCP Snooping credible port, all the response messages to the ports mentioned above will be dropped.

If the configuration above still can not help, please examine if the equipment that opened DHCP Snooping has opened router function, examine if the DHCP server address is correct.

Chapter 2 DHCP Server Configuration

This chapter is mainly about how to configure and maintain DHCP Server on the switch, including:

- ✧ DHCP Server principle overview
- ✧ DHCP Server configuration
- ✧ Monitoring and maintaining
- ✧ Typical configuration example
- ✧ DHCP Server trouble shooting

2.1 DHCP Server principle overview

Dynamic Host Configuration Protocol (DHCP) let the client acquire configuration information protocol in TCP/IP network, which is based on BOOTP protocol, and adds the function of automatic distribution useful network address and so on based on BOOTP protocol. The two protocol can make interoperability through some mechanism. DHCP offers the network hosts configuration parameters, which are made of two parts: one is to transmit special configuration information to network hosts, the other one is to assign network addresses to the hosts. DHCP is based on client/server mode, in this mode specific host assigns network addresses and transmits network configuration parameters to network hosts, the designated hosts are called server.

Usually, in the following situations DHCP server will be used to accomplish IP address distribution:

(1) When the network scope is too large for manual configuration or centralized management to the whole network.

(2) When the network host number is larger than the IP address number that the network supports, and can not give each host a stable IP address; there is also user number limit who can get into the network at the same time (for example, Internet access service provider belongs to the situation), lots of users have to acquire their own IP address dynamically from DHCP server.

(3) When there is not so many hosts who need stable IP address, and most hosts have no the need for stable IP address.

In typical DHCP application, there is usually one DHCP server and several client (like PC and portable machine), the typical DHCP application is shown below:

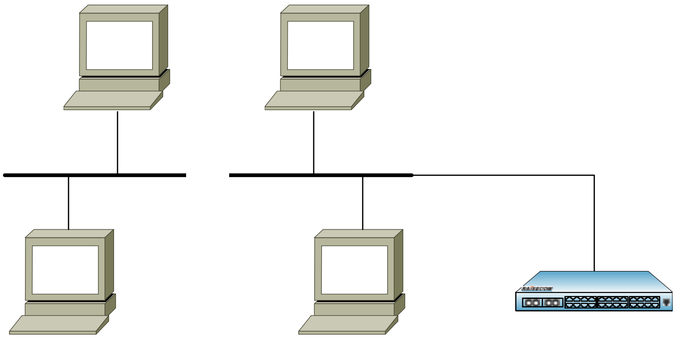

Fig 2-1 DHCP typical usage

2.2 Configure DHCP Server

This part is mainly about how to configure DHCP Server on the switch, including:

- ✧ Default DHCP Server configuration
- ✧ DHCP Server configuration guide
- ✧ Global DHCP Server configuration
- ✧ IP interface DHCP Server configuration
- ✧ Address pool configuration
- ✧ Lease table timeout configuration
- ✧ Border upon surrogate IP address configuration

⚠ Notice:

➢ Only ISCOM3000 serial switches support border upon surrogate IP address configuration.

2.2.1 Default DHCP Server configuration

Function	Default value
Global DHCP Server state	Disabled
IP port DHCP Server state	Disabled
Address pool	N/A
Lease table timeout	Maximum timeout: 1080 minutes Least timeout: 30 minutes Default timeout: 30 minutes
Neighbour proxy address	N/A

2.2.2 DHCP Server configuration guide

1. Make sure that DHCP Snooping on the switch is not on;

2. Global DHCP Server must be enabled;

3. If DHCP Server is not enable in IP port, DHCP Server does not take effect on this IP port;

4. When DHCP Server is on, DHCP Snooping can not be started either on the switch;

5. Make sure that the connection to DHCP Relay and DHCP server is correct, and the IP port address and the corresponding address pool range is correct.

6. If the client connect DHCP server through DHCP Relay, DHCP server must be ISCOM3000 serial switches. Except making sure IP port address and address pool configuration correct, correct configuration to neighbour proxy address and DHCP Relay.

2.2.3 Configure global DHCP Server

By default, global DHCP Server is disabled. Only when global DHCP Server is enabled, the switch DHCP Server can take effect. User can follow the steps below to start global DHCP Server:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp server**	Enable global DHCP Server
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp server**	Show DHCP Server configuration

⚠Notice

- If DHCP Snooping has been started on a switch, global DHCP Server can not be started any more.
- On the opposite, if global DHCP Server has been started, DHCP Snooping can not be started.

Use global configuration command **no ip dhcp server** to close global DHCP Server.

2.2.4 Configure IP port DHCP Server

By default, IP port DHCP Server function is disabled as well, user can use IP port command **ip dhcp server** to start IP port DHCP Server function. To close IP port DHCP Server, use IP port command **no ip dhcp server.**

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 4**	Enter IP port 4 configuration mode
3	**ip dhcp server**	Enable DHCP Server
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp server**	Show DHCP Server configuration

⚠ Notice:

- When global DHCP Server is off, user can start DHCP Server beforehand on a certain IP interface, but only when global DHCP Server starts, can the DHCP Server started from the IP port take effect.

2.2.5 Configure address pool

DHCP server selects and distributes IP address and other parameters from the address pool for the client. When the equipment that is selected as DHCP server receives a DHCP request from the client, it will select proper address pool by configuration, and then pick out a free IP address, which will sent out to the client together with other parameters (like DNS server address, address lease limit). Lots of standard configuration option is identified in RFC2132, where more detailed information can be got there. But most DHCP configurations use only a few options of the rules.

Following the steps below user can configure address pool:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**ip dhcp sever ip-pool WORD** *start-ip-address end-ip-address mask-address* **ip** *〈0-14〉* **[gateway** *ip-address* **] [dns** *ip-address* **] [secondary-dns** *ip-address* **]**	Configure the address pool
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp server ip-pool**	Show DHCP Server address pool configuration

⚠ Notice:

- The command can configure one address pool to IP interface once. If IP interface does not exist when configuring, still the address pool can be successfully configured, but it will not take effect until the IP port is created and the IP address is configured. If the IP port is changed or deleted, the configured address pool can still be kept. Once the IP port is re-created, the configured address pool will take effect again.
- If the client and the server is in the same subnet, when configuring IP address pool, the network section that the address pool is in should be the same with the network section that of IP port address's, that is to say, address pool's network address is the same with the port's network address; if the client connects the server through DHCP Relay, then the server's address and relay-ip should be within the same network section. Otherwise, DHCP Server will not distribute IP address for DHCP client.

Use global configuration command **no ip dhcp server ip-pool** ip-pool to delete the configured address pool. If the IP address pool that is to be deleted does not exist, returned value is fault.

Here, the maximum IP address pool number that can be configured for each IP port is 4, the maximum IP address number that the switch supports is 2500. Address pool take the name as the only mark.

Configuration example:

```
Raisecom#config

Raisecom(config)#ip dhcp server ip-pool pool1 192.168.1.100 192.168.1.200

255.255.255.0 ip 4 gateway 192.168.1.1 dns 192.168.1.1 secondary-dns 10.168.0.1

Raisecom(config)#exit

Raisecom#show ip dhcp server ip-pool
```

The result is shown below

```
-----------------------------------------------------------

Name of ip pool table : pool1

Status of IP pool table: active

IP address range: 192.168.1.100 - 192.168.1.200
```

Mask: 255.255.255.0

Including IP Interface: 4

IP address of gateway: 192.168.1.1

IP address of DNS server: 192.168.1.1

IP address of secondary DNS server: 10.168.0.1

Valid IP pool count : 1

Valid IP address count : 12

Allotted IP address count : 0

Gateway and dns is optical, if they are not used, default gateway and DNS will not be selected for the client.

2.2.6 Configure lease table timeout

When distributing IP address for the client, it is needed to designate the lease time of the IP address. By default the system lease time is:

1: default lease time: 30 minutes (usually it will not be used);

2: the maximum lease time: 10080 minutes (7days), when the lease time that the client requests is larger than this value, the larger value will be used.

3: the least lease time: 30 minutes, when the lease time that the client requests is smaller than this value, least lease time will be used; otherwise, according to the request time, if the client does not designate lease time, use the least lease time for distribution.

If the administrator needs to modify the least lease time, manual configuration is needed.

The configuration step is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2 (optical)	**ip dhcp sever default-lease** *timeout*	Configure the IP address pool default lease time for DHCP server
3 (optical)	**ip dhcp sever max-lease** *timeout*	Configure the IP address pool maximum lease time for DHCP serve
4 (optical)	**ip dhcp sever min-lease** *timeout*	Configure the IP address pool least lease time for DHCP serve
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp server**	Show DHCP server configuration

⚠ Notice:

- The lease time configured here is used for all the IP address of the address pool. At the same time, the maximum lease time can not be shorter than least rent time, default lease time must be between maximum and least lease time.

Use global command **no ip dhcp server default, no dhcp-server max-lease, no dhcp-server min-lease** to cannel the current setting, and restore system default lease time setting.

Configuration example:

```
Raisecom#config
Raisecom(config)#ip dhcp server default-lease 60
Raisecom(config)#ip dhcp server max-lease 1440
Raisecom(config)#ip dhcp server min-lease 45
Raisecom(config)#exit
Raisecom#show ip dhcp server
```

The result is shown below:

```
DHCP Server: Enabled
IP Interface Enabled: 4
Total Number: 1

Max lease time: 1440 m
Min lease time: 40 m
Default lease time: 60 m
```

2.2.7 Configure neighbour proxy IP address

When the client is connected with the server by DHCP Relay, DHCP server must know the neighbour DHCP Relay IP address, which needs the administrator’s manual configuration as well.

The configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp sever relay-ip** *ip-address ip-mask*	Configure neighbour proxy IP address
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp server relay-ip**	Show DHCP server configuration

⚠ Notice:

- Only ISCOM3000 serious switches support the command **ip dhcp server relay-op.** Here the configured neighbour proxy IP address is actually the port address that is connected with the client, as is shown in the typical example. The maximum number of neighbour proxy IP address is 8.

Use global configuration command **no ip dhcp server relay-ip** ip-address to delete neighbour proxy

IP address configuration.

Configuration example:

```
Raisecom#config
Raisecom(config)#ip dhcp server relay-ip 192.168.1.1 255.255.255.0
Raisecom(config)#exit
Raisecom#show ip dhcp server relay-ip
```

The result is shown below:

```
index   IP address         IP Mask          Status
-----------------------------------------------------------------
1        192.168.1.1         255.0.0.0          active
```

2.3 Monitoring and maintaining

Use different **show** commands to show the switch DHCP Server running and configuration situation for monitoring and maintaining. All the show commands are listed below:

Command	Description
show ip dhcp server	Show DHCP Server configuration and static information
show ip dhcp server ip-pool	Show DHCP Server address pool information
show ip dhcp server relay-ip	Show the configured neighbour DHCP proxy address information
show ip dhcp server lease	Show the designated IP address and the corresponding information

⚠ Notice:

- Only ISCOM3000 serial switches supports the command **show ip dhcp server relay-ip**
- Before using **show ip dhcp server lease,** the system time should better be configured accurately, because lease time limit is computed according to the system date absolute time.

Use **show ip dhcp server** command to look over the configuration information, like global or IP port configuration information, static information or so.

```
Raisecom#show ip dhcp server
In English:
DHCP Server: Enabled
IP Interface Enabled: 4
Total Number: 1

Max lease time: 1000 m
Min lease time: 32 m
Default lease time: 300 m
```

```
Statistics information:
Running time: 0 hours 7 minutes 33 seconds
Bootps: 0
Discover: 0
Request: 0
Release: 0
Offer: 0
Ack: 0
Nack: 0
Decline: 0
Information: 0
Unknows: 0
Total: 0
```

In Chinese:

```
DHCP 服务器: 启动
启动了 DHCP Server 的 IP 接口:   4
总数: 1

最大租赁时间: 1000  分钟
最小租赁时间: 32  分钟
缺省租赁时间: 300  分钟

统计信息:
运行时间:      0  小时  7  分钟  33  秒
Bootps: 0
Discover: 0
Request: 0
Release: 0
Offer: 0
Ack: 0
Nack: 0
Decline: 0
Information: 0
Unknows: 0
总共: 0
```

Use the command **show ip dhcp server ip-pool** to show the configured address pool information:

```
Raisecom#show ip dhcp server ip-pool
```

In English:

```
----------------------------------------------------
Name of IP pool table: dhcp
Status of IP pool table: active
IP address range: 11.1.1.33 - 11.1.1.44
Mask: 255.255.255.0
Including IP Interface: 4
IP address of gateway: 0.0.0.0
IP address of DNS server: 0.0.0.0
IP address of secondary DNS server: 0.0.0.0
----------------------------------------------------

Valid IP pool count: 1
Valid IP address count: 12
Allotted IP address count: 0
```

In Chinese:

```
---------------------------------------------------
```

```
地址池表项的名称: dhcp
地址池表项的状态: active
IP 地址范围:11.1.1.33-11.1.1.44
掩码: 255.255.255.0
包括的 IP 接口: 4
网关的 IP 地址: 0.0.0.0
DHCP DNS 服务器的 IP 地址: 0.0.0.0
DHCP  备用 DNS 服务器的 IP 地址: 0.0.0.0
-----------------------------------------------------

有效的地址池表项数目: 1
有效的 IP 地址数目: 12
已经分配的 IP 地址数目: 0
```

Use the command **show ip dhcp server relay-ip** to show the configured neighbour proxy address information:

```
Raisecom#show ip dhcp server relay-ip
```

In English:

```
Index IP Address             IP Mask                 Status
-----------------------------------------------------------------------
1         11.1.1.34              255.255.255.0           active
```

In Chinese:

```
Raisecom#show ip dhcp server relay--ip
序号      IP 地址                  IP 掩码          状态
----------------------------------------------------------------------
1         11.1.1.34              255.255.255.0           active
```

Use the command **show ip dhcp server lease** to show the configured neighbour proxy address information

```
Raisecom#show ip dhcp server lease
```

In English

```
IP Address            Hardware Address      Lease Expiration         IP Interface
--------------------------------------------------------------------------------------------
172.16.1.11           00:a0:98:02:32:de      Feb-01-2006 11:40:00         1
172.16.3.254          02:c7:f8:00:04:22      Jul-01-2006 23:00:00          1
```

In Chinese:

```
IP  地址                 硬件地址              租约到期时间              IP接口
--------------------------------------------------------------------------------------------
172.16.1.11           00:a0:98:02:32:de      Feb-01-2006 11:40:00         1
172.16.3.254          02:c7:f8:00:04:22      Jul-01-2006 23:00:00          1
```

Character instruction:

IP Address: the client IP address;

Hardware Address: the client MAC address

Lease Expiration: lease timeout limit

IP Interface: IP interface number

Lease timeout limit is computed according to system date, format is mm-dd-yyy hh:mm:ss

2.4 Typical configuration example

The typical DHCP Relay and Server configuration case is show below:

- Direct connection to the client for IP address
- The client get IP address through proxy

1) Configuration instruction

The example is simple and typical in realizing DHCP protocol. Specific connection state is shown in fig 2-2. In the figure ISCOM3026, as DHCP Relay, divides the two VLAN: VLAN 10 and VLAN 20, the two corresponding subnet IP address are 192.168.1.10 and 172.168.1.10 respectively. The DHCP server is ISCOM3026A, IP address is 172.168.1.2, suppose the subnet NDS be 172.168.1.3, subnet 1and subnet 2 need to get connection to public network through gateway 172.168.1.1. To realize the client accessing the resource of the public network, it is only needed to configure DHCP Server and DHCP Relay correctly.

2) Topology figure

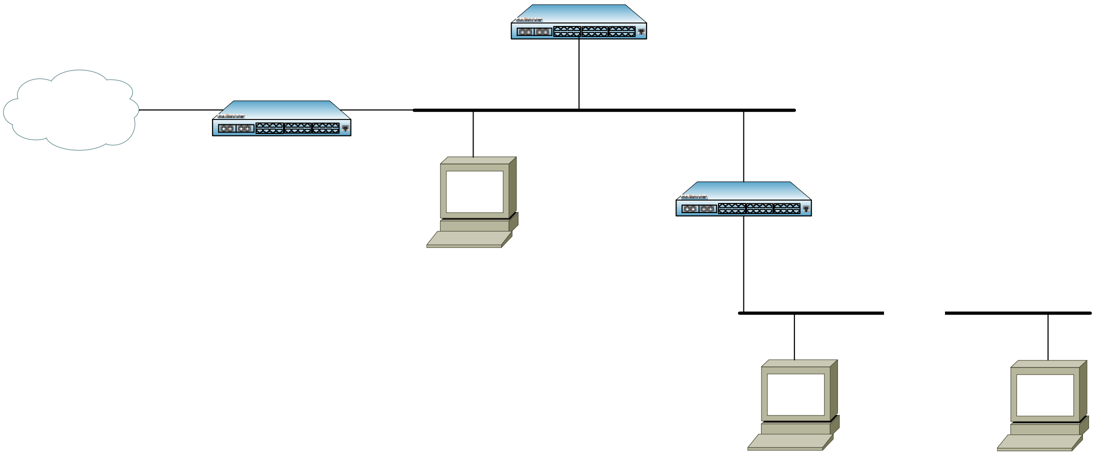

Fig 2-2 typical configuration example

3) Configuration steps

Configure DHCP Server:

- ➢ Configure VLAN and interfaces:

```
Raisecom(config)#create vlan 20 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport access vlan 20
Raisecom(config-port)#exit
Raisecom(config)#interface ip 2
Raisecom (config-ip)#ip address 172.168.1.2 255.255.0.0 20
```

ISCOM 2826
Gateway
172.168.1.1

Internet

- **Configure address pool**

Configuring a address pool for both subnet 1 and subnet 2 respectively.

```
Raisecom (config)#ip dhcp server ip-pool pool1 172.168.1.100 172.168.1.200 255.255.0.0 ip 2 gateway 172.168.1.1 dns 172.168.1.3
Raisecom(config)#ip dhcp server ip-pool pool2 192.168.1.100 192.168.1.200 255.255.255.0 ip 2 gateway 172.168.1.1 dns 172.168.1.3
Raisecom (config)#exit
Raisecom #show ip dhcp server ip-pool
```

- Start DHCP Server service

```
Raisecom (config)#ip dhcp server
Raisecom(config)#interface ip 2
Raisecom(config-ip)#ip dhcp server
Raisecom #show ip dhcp server
```

- Configure neighbour proxy IP address

```
Raisecom (config)#ip dhcp server relay-ip 192.168.1.10 255.255.255.0
Raisecom (config)#exit
Raisecom #show ip dhcp server relay-ip
```

- Configure the router

```
Raisecom (config)#ip route 192.168.1.0 255.255.255.0 172.168.1.10
```

- Configure DHCP Relay

Create VLAN and the interface

```
Raisecom (config)#create vlan 10 active
Raisecom (config)#interface port 1
Raisecom(config-port)#switchport access vlan 10
Raisecom(config-port)#exit
Raisecom (config)#interface ip 2
Raisecom(config-ip)#ip address 192.168.1.10 255.255.255.0 10
Raisecom (config)#create vlan 20 active
Raisecom (config)#interface port 2
Raisecom(config-port)#switchport access vlan 20
Raisecom(config-port)#exit
Raisecom (config)#interface ip 3
Raisecom (config-ip)#ip address 172.168.1.10 255.255.0.0 20
```

- Enable router function

```
Raisecom(config-ip)#exit
Raisecom(config)#ip routing
```

- Configure DHCP server IP address

```
Raisecom(config)#ip dhcp relay ip-list 2 target-ip 172.168.1.2
Raisecom (config)#exit
Raisecom #show ip dhcp relay
```

- Start DHCP Relay

```
Raisecom (config)#ip dhcp relay
Raisecom(config)#exit
Raisecom #show ip dhcp relay
```

The client will be configured as auto acquiring IP address through DHCP

4) show the result

Show DHCP configuration static information, address pool information and the configured IP address information

On ISCOM3026A use the command **show ip dhcp server**、**show ip dhcp server ip-pool** and **show ip dhcp server lease**.

Show DHCP Relay information

On ISCOM3026B use the command **show ip dhcp relay**.

- Show client A

```
c:\>ipconfig /all
Ethernet adapter: local connection:
        Connection-specific DNS Suffix   . :
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-50-8D-4B-FD-27
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enable. . . :Yes
        IP Address. . . . . . . . . . . . : 172.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.168.1.1
        DHCP server. . . . . . . . . . . .: 172.168.1.2
        DNS Servers . . . . . . . . . . . : 172.168.1.3
        Lease Obtained. . . . . . . . . :2006 年 9 月 8 日 13:03:24
        Lease Expires. . . . . . . . . :2006 年 9 月 8 日  13:33:24
```

- Show client B

```
c:\>ipconfig /all
Ethernet adapter: local connection:
        Connection-specific DNS Suffix    . :
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-50-8D-4B-DE-46
        DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enable. . . :Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.168.1.1
        DHCP server. . . . . . . . . . . .: 172.168.1.2
        DNS Servers . . . . . . . . . . . : 172.168.1.3
        Lease Obtained. . . . . . . . . :2006 年 9 月 8 日 13:03:24
        Lease Expires. . . . . . . . . :2006 年 9 月 8 日  13:33:24
```

- Show client C:

Client C is the same with client B in content, the IP address is 92.168.1.101

Chapter 3 DHCP Relay Configuration

This chapter is mainly about how to configure and maintain DHCP Relay on the switch, including:

- ✧ DHCP Relay principle overview
- ✧ DHCP Relay configuration
- ✧ Monitoring and maintaining
- ✧ Typical configuration example
- ✧ DHCP Relay trouble shooting

3.1 DHCP Relay principle overview

Early DHCP protocol is suitable for only the situation that the client and server are in the same subnet, which can not go through network sections. Therefore, for dynamical host configuration, configuring a DHCP server on all the network sections is needed, which is obviously wasteful.

The introduction of DHCP Relay solves this problem: the local network client can communicate with the other subnet DHCP servers by DHCP Relay, and get the legal IP address finally. Thus, the DHCP client on several networks can use the same DHCP server, which decreases the cost and helps centralized management

DHCP Relay provides DHCP broadcast message transparent transmission function, which is able to transmit the broadcast message of DHCP client (or server) transparently to the other network section DHCP server (or client).

In the process that DHCP Relay completes dynamic configuration, the processing way that DHCP client and server takes is basically the same with that of not through DHCP Relay. The following steps are only about DHCP Relay transmission:

(1) DHCP client transmits DHCP-DISCOVER message in broadcasting.

(2) When the network equipment with DHCP Relay function receives the broadcast message, by configuration it will transmit the message to the specific DHCP server in unicast.

(3) DHCP server makes IP addresses distribution, and sends the configuration information to the client through DHCP Relay.

Usually, DHCP Relay can be either host or three-layer switch or router, if only DHCP Relay service program is enable.

The figure below is a typical DHCP Relay application:

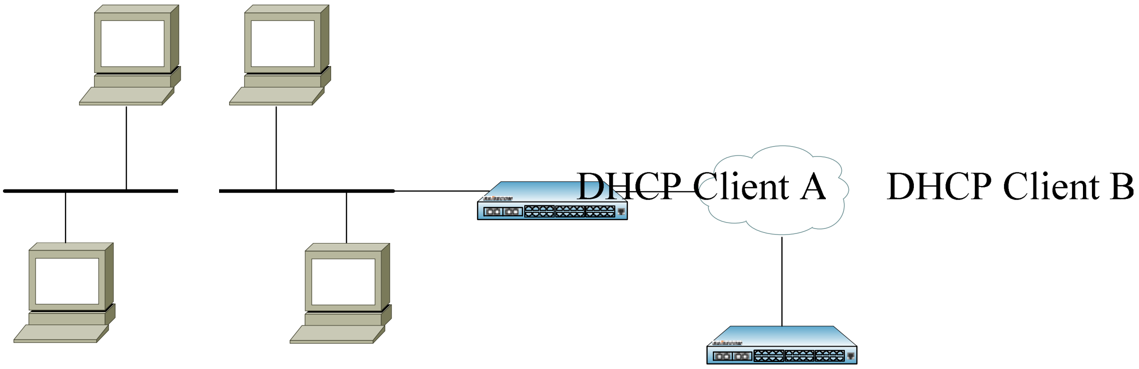

Fig 3-1 DHCP Relay typical application

The mechanism of DHCP Relay support Option 82 is shown below:

(1) DHCP client sends out request message in the form of broadcasting when initialized.

(2) The DHCP Relay equipment that is connected with local network will receive the broadcast message, check out if there has been Option 82 in the message, and handles it in the corresponding way.

(3) If there has been Option 82 in the message, the equipment will follow the configured strategy to handle the message (drop, replace the Option 82 in the message that has been there with the relay equipment's Option 82 or keep the Option 82 that has been there), and transmits the request message to DHCP server.

(4) If there is no Option 82 in the request message, the Option 82 of DHCP equipment will be added into the message (located in the end of all the options) and be transmitted to DHCP server. At this time, the Option 82 of the request message contains the port number of the switch which is connected with DHCP client, the number of the VLAN that the port belongs to and the DHCP Relay equipment's own MAC address and so on.

(5) When DHCP server receives the DHCP request message that is transmitted by DHCP Relay equipment, it will record the information from Option in the message, then transmit the message that contains DHCP configuration information and Option 82 information.

(6) After DHCP Relay receives the response message of DHCP server it will peel off the message's Option 82 information, then transmit the message that contains DHCP configuration information to DHCP client.

Explanation: there are two sorts of request messages from DHCP client, DHCP-DISCOVER and DHCP-REQUEST message. Because of the different mechanisms that different manufacturers' DHCP server handle request messages, some equipments handle DHCP-DISCOVER message's Option 82 information, while some others handle DHCP-REQUEST message's Option 82 information, so DHCP Relay handles both the two messages in the strategy of Option 82.

Otherwise, if DHCP Relay receives the messages sent out from the two DHCP client DHCP-DECLINE and DHCP-INFORM, it will handle Option 82 uniformly according to the strategy, without affecting its basic function of supporting Option 82.

3.2 Configure DHCP Relay

This part is about how to configure DHCP Relay on the switch, including the following configuration information:

- ✧ Default DHCP Relay configuration
- ✧ DHCP Relay configuration guide
- ✧ Global DHCP Relay configuration
- ✧ IP port DHCP Relay configuration
- ✧ DHCP Relay support Option 82 configuration
- ✧ DHCP Relay’s handling strategy to the request messages that contains option 82 configuration
- ✧ Port DHCP Relay trust configuration

3.2.1 Default DHCP Relay configuration

The following table is the default configuration steps of DHCP Relay:

Function	Default value
Global DHCP Relay state	Disabled
IP port DHCP Relay state	Enabled
IP port’s destination IP address	N/A
DHCP Relay support Option 82	Disabled
The strategy of DHCP Relay handling option 82 request messages	Replace
Port DHCP Relay trust	Untrusted

3.2.2 DHCP Relay configuration guide

1. Make sure the DHCP Snooping on the switch is not started;

2. Global DHCP Relay must be started;

3. If on a IP port DHCP Relay is not started, it can not work on this IP port;

4. When DHCP Relay is on, DHCP Snooping can not be started either on the switch;

5. Make sure the DHCP server that is connected with DHCP Relay has correct configuration and connection to the client. DHCP server must be ISCOM 3000 serious switches. Except making sure the correct configuration of IP port addresses and address pool, correct configuration to the neighbour proxy address and Relay addresses;

6. If the client acquires IP address automatically from DHCP server through multiplex Relay, you must make sure the connection of each equipment and correct configuration. The DHCP Relay number between the client and server, can not exceed 16 in RFC1542 rules, it is usually suggested not to exceed 4.

3.2.3 Configure global DHCP Relay

By default, global DHCP Relay is off. Only when global DHCP Relay is on can the switch DHCP Relay takes effect. User can take the following steps to start global DHCP Relay.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay**	Start global DHCP Relay
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp relay**	Show DHCP Relay configuration

⚠ Notice:

➢ If the switch starts DHCP Snooping, it can not start global DHCP Relay. On the opposite, if the switch starts global DHCP Relay, it can not start DHCP Snooping.

Use global command **no ip dhcp relay** to disable global DHCP Realy.

3.2.4 Configure IP port DHCP Relay

By default, IP port DHCP Relay function is on, user can use IP port command **no ip dhcp relay** to disable IP port DHCP Relay function. To start IP port DHCP Relay, use IP port command **ip dhcp relay.**

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 4**	Enter IP port 4 configuration mode
3	**ip dhcp relay**	Start DHCP Relay
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp relay**	Show DHCP Relay configuration

⚠ Notice:

➢ When global DHCP Relay is off, on a certain IP port DHCP Relay can be started in advance. But only when global DHCP Relay starts can the DHCP Relay started on this port takes effect.

3.2.5 Configure IP port destination IP address

When the client equipment and DHCP server is not in the same broadcasting domain, the relay equipment in the middle must be able to transmit the kind of broadcasting packet. Configuring the destination IP address of DHCP Relay points out the destination address of the DHCP broadcasting packet from DHCP client for the relay equipment.

When DHCP Relay is configuring destination IP address, use network port LIST for the convenience of user’s configuration. That is to say, according to the actual need, one command can be used to configure the same IP address for parts of the network ports or all the ports.

When DHCP Relay is configuring destination IP address, except the configuration commands in config mode, you can also configure the port's corresponding destination IP address in IP port, which is flexible.

Take the following steps to configure the port's destination IP address.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay ip-list all target-ip** *10.199.0.200*	For all the IP ports configure the destination IP 10.199.0.200
3	**ip dhcp relay ip-list** *1-3* **target-ip**	For IP port 1-3 configure the destination IP 10.200.0.200
4	**interface ip** *3*	Enter IP port 3 configuration mode
5	**ip dhcp relay target-ip**	Configure the destination IP 10.201.0.200
6	**exit**	Return to global configuration mode

⚠Notice:

- Here, the configured maximum destination IP address number for each port is 4. At the same time, make sure that the destination IP address is correct.
- When it comes to configuring destination IP address for several IP ports in one command, if configuring the destination IP address in a certain port fails, the rest IP port destination IP address configuration should be continued and return the cue which specific port configuring destination IP address fails, the format is: IP interface %s set target IP address unsuccessfully. Use IP table to replace %s in actual use. If only one port is configured successfully, the command line will return 'configuration successful' finally.

Use global configuration command **no ip dhcp relay ip-list target-ip** to delete the configured destination IP address of the IP port, or IP interface configuration command **no ip dhcp relay target-ip** in the corresponding port configuration mode.

Configuration example:

```
Raisecom#config

Raisecom(config)# ip dhcp relay ip-list all target-ip 10.199.0.200

Raisecom(config)# ip dhcp relay ip-list 1-3 target-ip 10.200.0.200

Raisecom(config)#interface ip 3

Raisecom(config-ip)#ip dhcp relay target-ip 10.201.0.200

Raisecom(config-ip)#exit

Raisecom(config)#exit

Raisecom#show ip dhcp relay
```

The result is shown below:

```
DHCP Relay: Enabled


IP Interface     Enabled Status    Target IP Address

----------------------------------------------------------

0               enabled           10.199. 0.200

1               enabled           10.199. 0.200
```

```
10.200.0.200
2          enabled         10.199. 0.200
10.200.0.200
3          enabled         10.199. 0.200
10.200.0.200
10.201.0.200
4          enabled         10.199. 0.200
…           …               …
…           …               …
```

3.2.6 Configure DHCP Relay support option 82

By default, DHCP Relay do not support option 82, in global configuration mode use **ip dhcp relay information option** to start DHCP Relay support option 82.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay information**	Start DHCP Relay support option 82
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp relay information**	Show DHCP Relay support Option 82 configuration information and port trust list

⚠Notice:

- To active DHCP Relay support option 82, enable global DHCP Relay service first. To make option 82 function available, corresponding configuration on DHCP Server is needed.

Use global configuration command **no ip dhcp relay information option** to disable DHCP Relay support Option 82.

3.2.7 Configure DHCP Relay request message handling strategy

By default, DHCP Relay handling strategy to the client request messages is Replace, that is to fill Option 82 in the way of normal or verbose, replace the Option 82 contents that has been there and transmit it. In global configuration mode use the command **ip dhcp relay information policy {drop| keep | replace}** to configure the message handling strategy of DHCP Relay as drop, keep or replace.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay information policy {drop |**	Configure DHCP Relay request message

	keep | replace} [**schedule-list** *list-no*]	handling strategy
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp relay information**	Show DHCP Relay handling strategy to client request message

⚠ Notice:

- The command configured request message handling strategy can available only in DHCP Relay support Option 82.

  Use global configuration command **no ip dhcp relay information policy {drop | keep | replace} [schedule-list** *list-no***]** to recover default DHCP Relay handling strategy to Option 82.

  The configuration example:

```
Raisecom#config
     Raisecom(config) ip dhcp relay information policy keep
     Raisecom(config)#exit
     Raisecom#show ip dhcp relay information
```

  the result is shown below:

  In English:

```
Option 82: Enabled
Policy: Keep

Port                 Trusted
------------------------------
…                        …
```

  In Chinese:

```
Option 82: Enabled
Policy: Keep

端口                 信任
------------------------------
…                        …
```

3.2.8 Port DHCP Relay trust configuration

By default, if one DHCP message gateway address part is 0 and relay agent information option part (option 82) exists, then DHCP Relay will drop messages of this kind. If DHCP Relay is required to transmit messages of this kind, use the command to configure DHCP Relay port trust. After the specific port has configured DHCP Relay port trust command, these port can transmit this kind of DHCP messages normally. You can also use the key word all to set all the system port Relay Agent Information Option port trust.

When configuring port trust, except the configuration commands in config mode, you can configure the port trust state under the port directly as well, which is flexible.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay information trusted port-list** *1-7*	Set port 1-7 to trusted port
3	**interface ip** *8*	Enter port 8 configuration mode
4	**ip dhcp relay information trusted**	Configure the destination IP 10.201.0.200
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show ip dhcp relay information**	Show DHCP Relay support Option 82 configuration information and port trust table

⚠ Notice:

- Only when DHCP Relay support Option 82 can port trust take effect.

Use global configuration command **no ip dhcp relay information port-list** to set the port to distrust port, in the corresponding port configuration mode use port configuration command **no ip dhcp relay information option** to realize it.

Configuration example:

```
Raisecom#config
Raisecom(config) ip dhcp relay information trusted port-list 1-7
Raisecom(config)#interface ip 8
Raisecom(config-port)# ip dhcp relay information trusted
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show ip dhcp relay information
```

The result is shown below:

```
Option 82: Disabled

Policy: Replace


Port                Trusted

------------------------------

1                     yes

2                     yes

3                     yes

4                     yes

5                     yes

6                     yes

7                     yes

8                     yes

…                     …

…                     …
```

3.3 Monitoring and maintaining

Use different show commands to show switch DHCP Relay running state and configuration state for monitoring and maintaining. All the show commands are listed below:

Command	Description
show ip dhcp relay	Show DHCP Relay configuration information
show ip dhcp relay statistics	Show DHCP Relay static.
show ip dhcp relay information	Show the configured neighbour DHCP proxy address information

Use the command **show ip dhcp relay** to show HDCP Relay basic configuration information, including DHCP Relay state, IP port DHCP Relay state and the corresponding DHCP proxy destination IP address.

```
Raisecom#show ip dhcp relay
In English:
DHCP Relay: Enabled

IP Interface     Enabled Status    Target IP Address
---------------------------------------------------------
  0               enabled            10.199. 0.200
  1               enabled            10.199. 0.200
                                     10.200.0.200
  2               enabled            10.199. 0.200
```

```
                              10.200.0.200
 3          enabled            10.199. 0.200
                              10.200.0.200
                              10.201.0.200
 4          enabled            10.199. 0.200
 …             …                  …
 …             …                  …

In Chinese:
DHCP Relay: Enabled

IP 接口         使能状态          目的 IP 地址
-----------------------------------------------------
 0          enabled            10.199. 0.200
 1          enabled            10.199. 0.200
                              10.200.0.200
 2          enabled            10.199. 0.200
                              10.200.0.200
 3          enabled            10.199. 0.200
                              10.200.0.200
                              10.201.0.200
 4          enabled            10.199. 0.200
 …             …                  …
 …             …                  …
```

Use the command **show ip dhcp relay statistics** to show DHCP Relay static, including DHCP Relay running time and received/sending messages number.

Raisecom#**show ip dhcp relay ip-pool**

```
In English:
Runtime:         0 hours 23 minutes 34 seconds

Packet Type      Receive      Send
------------------------------------------
Bootp              0            0
Discover           1            1
Request            1            1
Decline            0            0
Offer              0            0
Ack                0            0
Nack               0            0
Decline            0            0
Inform             0            0
Unknowns           0            0

Total                2              2

In Chinese:
运行时间：    0  小时  23  分钟  34  秒

报文类型        接收            发送
------------------------------------------
Bootp              0            0
Discover           1            1
Request            1            1
Decline            0            0
Offer              0            0
```

```
Ack               0              0
Nack              0              0
Decline           0              0
Inform            0              0
Unknowns          0              0

Total             2              2
```

Use the command **show ip dhcp relay information** to show HDCP Relay support Option 82 configuration information and port trust table:

```
Raisecom#show ip dhcp relay information
```

In English:

```
Option 82: Enabled
Policy: Replace

  Port              Trusted
  ------------------------------
  1                   yes
  2                   no
  3                   yes
  4                   yes
  …                   …
```

In Chinese:

```
Raisecom#show ip dhcp relay relay--ip
Option 82: Enabled
Policy: Replace

    端口              信任
    ------------------------------
    1                   yes
    2                   no
    3                   yes
    4                   yes
    …                   …
```

Instruction:

DHCP Relay supporting Option 82 includes:

a) Enabled

b) Disabled

The strategy includes:

a) Drop

b) Keep

c) Replace

3.4 Typical configuration example

DHCP Relay typical configuration example is like DHCP Server typical configuration example. The following is about a example that the client using DHCP Snooping connects to DHCP Relay and get IP address.

1) Configuration instruction

1: the connection of starting Snooping on DHCP Snooping equipment is as fig 3-2, start DHCP Snooping support option 82, and set port 2 to DHCP Snooping trust port.

2: DHCP Relay divides two subnets, the connection between it and the client and the server connection and configuration is as the figure below. Follow the figure to configure VLAN, IP port address and the VLAN that the port belongs to.

3: DHCP Server divides two subnets, establish correct address pool (10.150.0.2 – 10.150.0.100) on the subnet, start DHCP Server function at the same time and configure relay-ip shown in the figure (consult DHCP Server module configuration guide). Then follow the figure to configure VLAN, IP port address and VLAN the port belongs to, and configure it to the router belongs to 10.150 network segment.

4: set PCI to auto acquiring IP address.

2) Topology figure

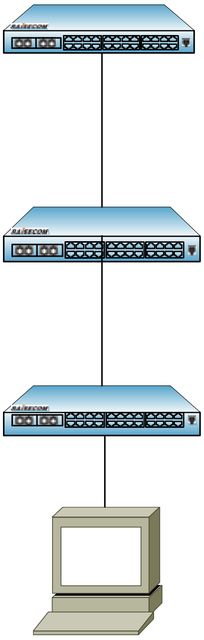

Fig 3-2 typical configuration example

3) Configuration steps:

Configure DHCP Relay:

- Start global DHCP Relay

```
Raisecom (config)#ip dhcp relay
```

- Prot 14 configure destination IP addresss

```
Raisecom (config)# ip dhcp relay ip-list 14 target-ip 10.168.0.199
```

- Start DHCP Realy support option 82

```
Raisecom (config)ip dhcp relay information option
```

- Configure port 1 as DHCP Relay trust port

```
Raisecom (config)ip dhcp relay information trusted port-list 1
```

10.168.0.20
Port 5/ VLA
/ IP0

- Open the router function

```
Raisecom (config)#ip dhcp relay ip routing
```

a) show the result

- Show the client PC1

```
C:\>ipconfig /all
Ethernet adapter local connection
        Connection-specific DNS Suffix    . :
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-50-8D-4B-FD-27
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enable. . . :Yes
        IP Address. . . . . . . . . . . . : 10..150.0.0
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
        DHCP server. . . . . . . . . . . . .: 10.168.0.199
        DNS Servers . . . . . . . . . . . :
        Lease Obtained. . . . . . . . . :2007 年 4 月 8 日 13:03:24
        Lease Expires. . . . . . . . . :2007 年 4 月 8 日  13:33:24
```

3.5 DHCP Relay trouble shooting

1. If the correct destination IP address is not designated, DHCP Relay can not transmit the message correctly.

2. If the gateway address field of a DHCP message is 0 and relay agent information option field exists, DHCP Relay distrusted port will drop messages of this kind.

If the configuration above still can not help, please examine if DHCP Relay has started router function, and examine if DHCP server address is correctly configured, if the neighbour proxy default gateway or router is configured.

北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road, Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com http://www.raisecom.com